高等院校网络空间安全专业实战化人才培养系列教材

郭启全　丛书主编

网络安全威胁情报分析与挖掘技术

薛　锋　郭启全　樊兴华　于海洋　鲁玮克
温佳宝　张　征　李元富　张　宽　编著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书共 7 章，主要介绍威胁情报的起源、价值以及威胁情报的分析与挖掘的基本含义，威胁情报的基本概念和相关基础知识，网络安全领域常见的网络攻击技术，威胁情报相关技术，威胁情报的关键挖掘体系，包括情报生产、质量测试、过期机制等核心技术，结合具体案例介绍威胁情报挖掘的典型流程实践和建立高价值的攻击者画像的相关方法，如何应用和管理威胁情报，威胁情报在国家、行业以及企业的典型应用场景，并介绍行业内的应用实践案例。最后介绍了大语言模型技术在网络安全威胁情报分析与挖掘技术威胁情报分析与挖掘中的应用。

本书是高等院校网络空间安全专业实战化人才培养系列教材之一，可作为网络空间安全专业的专业课教材，适合网络空间安全专业、信息安全专业以及相关专业的大学生、研究生系统学习，也适合各单位各部门从事网络安全工作者、科研机构和网络安全企业的研究人员阅读。

图书在版编目（CIP）数据

网络安全威胁情报分析与挖掘技术 / 薛锋等编著.
北京 : 电子工业出版社, 2025. 7. -- ISBN 978-7-121
-50323-8

Ⅰ. TP393.08；G252.8

中国国家版本馆CIP数据核字第2025M577N4号

责任编辑：刘御廷　　文字编辑：李　安
印　　刷：
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路173信箱　　邮编：100036
开　　本：787×1 092　1/16　印张：16　　字数：384千字
版　　次：2025年7月第1版
印　　次：2025年7月第1次印刷
定　　价：69.00元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

本书咨询联系方式：lyt@phei.com.cn。

高等院校网络空间安全专业
实战化人才培养系列教材

编委会

序 FOREWORD

在数字化智慧化高速发展的今天，网络和数据安全的重要性愈发凸显，直接关系到国家政治、经济、国防、文化、社会等各个领域的安全和发展。网络空间技术对抗能力是国家整体实力的重要方面，面对日益复杂的网络安全威胁和挑战，按照“打造一支攻防兼备的队伍，开展一组实战行动，建设一批网络与数据安全基地”的思路，培养具有实战化能力的网络安全人才队伍，已成为国家重大战略需求。

一、培养网络安全实战化人才的根本目的

在网络安全“三化六防”（实战化、体系化、常态化；动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控）理念的指引下，网络安全业务越来越贴近实战。实战行动和实战措施都离不开实战化人才队伍的支撑。培养网络安全实战化人才的根本目的，在于培养一批既具备扎实的理论基础，又掌握高新技术和前沿技术、具备攻防技术对抗能力，还能灵活运用各种技术措施和手段，应对各种网络安全威胁的高素质实战化人才，打造“攻防兼备”和具有网络安全新质战斗力的队伍，支撑国家网络安全整体实战能力的提升。

二、培养网络安全实战化人才的重大意义

习近平总书记强调：“网络空间的竞争，归根结底是人才竞争”，“网络安全的本质在对抗，对抗的本质在攻防两端能力较量”。要建设网络强国，必须打造一支高素质的网络安全实战化人才队伍。我国网络安全人才特别是实战化人才严重缺乏，因此，破解难题，从网络安全保卫、保护、保障三个方面加强实战化人才教育训练，已成为国家重大战略需求。

当前，国家在加快推进数字化智慧化建设，本质是打造数字化生态，而数字化建设面临的最大威胁是网络攻击。与此同时，国家网络安全进入新时代，新时代网络安全最显著的特征是技术对抗。因此，新时代要求我们要树立新理念、采取新举措，从网络安全、数据安全、人工智能安全等方面，大力培养实战化人才队伍，加强“网络备战”，提升队伍的技术对抗和应急处突能力，有效应对新威胁和新技术带来的新挑战，为国家经济发展保驾护航。

三、构建新型网络安全实战化人才教育训练体系

为全面提升我国网络安全领域的实战化人才培养能力和水平，按照“理论支撑技术、技术支撑实战”的理念，创新高等院校及社会差异化实战人才培养的思路和方法，建立新型实战化人才教育训练体系。遵循“问题导向、实战引领、体系化设计、督办落实”四项原则，认真落实“制定实战型教育训练体系规划、建设实战型课程体系、建设实战型师资队伍、建设实战型系列教材、建设实战型实训环境、以实战行动提升实战能力、创新实战

型教育训练模式、加强指导和督办落实”八项重大措施，形成实战化人才培养的“四梁八柱”，有力提升网络安全人才队伍的新质战斗力。

四、精心打造高等院校网络空间安全专业实战化人才培养系列教材

在有关部门的大力支持下，具有 20 多年网络安全实战经验的资深专家统筹规划和整体设计，会同 20 多位部委、高等院校、科研机构、大型企业具有丰富实战经验和教学经验的专家学者，共同打造了 14 部技术先进、案例鲜活、贴近实战的高等院校网络空间安全专业实战化人才培养系列教材，由电子工业出版社出版，以期贡献给读者最高水平、最强实战的网络安全重要知识、核心技术和能力，满足高等院校和社会培养实战化人才的迫切需要。

网络安全实战化人才队伍培养是一项长期而艰巨的任务，按照教、训、战一体化原则，以国家战略为引领，以法规政策标准为遵循，以系统化措施为抓手，政府、高校、企业和社会各界应共同努力，加快推进我国网络安全实战化人才培养，为筑梦网络强国、护航中国式现代化贡献我们的智慧和力量！

郭启全

前言 PREFACE

随着网络技术的不断进步和应用领域日益广泛，网络安全已成为全球关注的焦点，全球网络安全事件频发，数据泄露、业务中断等事件时有发生，网络安全威胁的范围与内容不断扩大和演化，呈现出多样化、复杂化特点。为了应对不断演进的网络安全威胁和风险，网络安全行业逐步从“被动防御”转向“主动防御”，威胁情报这一全新的技术和理念应运而生，并逐渐得到重视和应用，威胁情报的价值已经被重点行业和大型企业普遍认可。近年来，威胁情报逐渐成为网络安全的热点领域之一，各国政府、企业对威胁情报的重视程度不断提高，未来的网络安全不仅仅是防御攻击，更重要的是通过主动收集和分析威胁情报，预测并应对潜在的安全威胁。

进入新时代，网络安全最显著的特征是技术对抗，应树立新理念，采取新举措，立足有效应对大规模网络攻击，认真落实“实战化、体系化、常态化”和“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”的“三化六防”措施，按照“打造一支攻防兼备的队伍，开展一组实战演习行动，建设一批网络与数据安全基地”这条主线，加强战略谋划和战术设计，建立完善的网络安全综合防御体系，大力提升综合防御能力和技术对抗能力。

为了满足培养网络安全实战型人才需要，由郭启全组织成立编委会，共同编著高等院校网络空间安全专业实战化人才培养系列教材，包括《网络安全保护制度与实施》《网络安全建设与运营》《网络空间安全技术》《商用密码应用技术》《数据安全管理与技术》《人工智能安全治理与技术》《网络安全事件处置与追踪溯源技术》《网络安全检测评估技术与方法》《网络安全威胁情报分析与挖掘技术》《数字勘查与取证技术》《恶意代码分析与检测技术》《恶意代码分析与检测技术实验指导书》《漏洞挖掘与渗透测试技术》《网络空间安全导论》。全套教材由郭启全统筹规划和整体设计，组织具有丰富网络安全实战经验和教学经验的专家、学者撰写，并对内容严格把关，以期贡献给读者一套最高水平、最强实战的网络安全、数据安全、人工智能安全等方面的优秀教材。

《网络安全威胁情报分析与挖掘技术》一书共 7 章，主要介绍威胁情报的起源、价值以及威胁情报的分析与挖掘的基本含义，威胁情报的基本概念和相关基础知识，网络安全领域常见的网络攻击技术，威胁情报相关技术，威胁情报的关键挖掘体系，包括情报生产、质量测试、过期机制等核心技术，结合具体案例介绍威胁情报挖掘的典型流程实践和建立高价值的黑客画像的相关方法，如何应用和管理威胁情报，威胁情报在国家、行业以及企业的典型应用场景，并介绍行业内的应用实践案例。最后介绍了大语言模型技术在威

胁情报分析与挖掘中的应用。

本书第 1、2、3 章由于海洋、薛锋撰写，第 4 章由温佳宝、李元富、鲁玮克撰写，第 5 章由鲁玮克撰写，第 6 章由张宽撰写，第 7 章由樊兴华撰写。全书由郭启全设计和组织，由郭启全、张征、樊兴华统稿。

书中不足之处，敬请读者指正。

作者

目录 CONTENTS

第 3 章

常见网络攻击技术

第 1 章 概述

本章介绍威胁情报的起源、威胁情报的价值、威胁情报分析与挖掘的相关概念，从《孙子兵法》中的情报观、美国军事情报理论中的情报观出发，研究探讨网络安全威胁情报观，威胁情报守护企业安全、社会安全和国家安全，威胁情报分析与挖掘的过程、技术和方法、效果评估及策略等内容，使读者建立起网络安全威胁情报的概念。

1.1 威胁情报的起源

情报学作为一门现代学科，自第二次世界大战后迅速发展，但情报的历史最早可追溯到中国的东周时期。《孙子兵法》中体现出了朴素、实用的情报观，引领了当时乃至后世情报观的进步，而在以美国为代表的西方国家中，情报观也经历了不断的完善和进化。分析古今中外的情报观进化史，能在系统性研究网络安全威胁情报之前，形成对网络安全威胁情报的最基础认识。

1.1.1 《孙子兵法》中的情报观

《孙子兵法》阐述了军事情报和战争决策的关系。《孙子兵法》将古典政治情报理论运用在更细分的军事领域，并根据军事领域的特征将情报理论进行了体系化、专业化的延伸，形成了朴素的战略情报、战役/战场情报、战术情报的分析方法和认识论。

孙子认为，情报应当具备准确性、及时性，能够为军事行动提供保障。在进行情报获取和分析时，应重视人的主观能动作用，主张由此及彼、由表及里的分析方式，反对经验主义和机械推理。此外，《孙子兵法》的情报思想包括“知己”和“知彼”两部分，主张对自身与敌方的信息归类成项，经过逐项分析、对比分析后，再进行综合评估，整个过程奠定了中国古典军事战略情报分析流程的形制。

作为世界上现存最早的军事理论著作，《孙子兵法》被各国的军事理论研究者广泛学习，书中提出的情报理论在 2000 多年后仍然具有很强的适用性。在现代战争中形成的情报观，亦能与《孙子兵法》相呼应。

1.1.2 美国军事情报理论中的情报观

美国的信息战能力强、经验丰富。美国的军事情报理论对英国、加拿大、澳大利亚等西方国家产生了深刻影响。研究美国军事情报理论的发展历史和现状，能大致掌握在现代战争中形成并不断完善的现代情报观。

美国情报理论先驱谢尔曼·肯特曾在《服务于美国世界政策的战略情报》一书中对情报提出三个定义，分别是“情报即知识”（Intelligence is knowledge），“情报即组织”（Intelligence is organization），“情报即行动”（Intelligence is activity）。在肯特看来，情报需要包含知识、组织和行动三要素。同时，肯特提出了“战略情报”的概念，认为情报是“战略家拟定并执行计划必须掌握的东西”，是“身居高位的文武官员保卫国家福祉必须掌握的知识”，这一观点与孙子提出的“庙算”不谋而合。

肯特以时间为根本要素，创造性地将战略情报所要获取的信息划分为基本描述型（basic descriptive form）、现实报告型（current reportorial form）和预测评价型（speculative-evaluative form）三种类型，分别对应过去、现在和未来。阿布拉姆·萨尔斯基、迈克尔·汉德尔等学者先后对肯特的学说进行了扩充和完善。

美国文职部门和军方有关情报的定义明显反映出了对上述学者不同观点的吸收，接受了肯特“情报即知识”的表述，且更加强调了情报预测的重要性，同时在《情报改革及防止恐怖主义法》中也建议成立专门的情报中心，以协调整个情报界开源情报的搜集、分析、生产和分发。这与肯特“情报即组织”和“情报即行动”的表述也是吻合的。此外，美国官方强调对情报进行分析的必要性，认为“情报 = 信息 + 分析的结果”，经过分析的情报能够有力地辅助决策。

1.1.3 开展网络安全威胁情报工作的原则

应从维护国家安全、社会公共安全、人民群众合法权益出发，围绕保护关键信息基础设施、重要网络和大数据安全，针对敌对势力、黑客组织和不法分子等攻击者，按照着手于攻击端、被攻击端和攻击路径的“两端一路”思路，开展网络安全威胁情报搜集和分析研判工作，形成有价值的威胁情报，为公安机关打击网络违法犯罪和重要领域网络安全防御提供支撑，坚持以下原则。

（1）掌握“攻击端”情况，即搞清攻击者基本情况，包括敌对势力、黑客组织、犯罪团伙和不法分子等，掌握相关组织的背景、架构、人员情况、活动情况，建设黑客档案库，做到知己知彼。

（2）掌握“被攻击端”情况，即搞清我国哪些地区、行业、部门是敌对势力、黑客组织、犯罪团伙和不法分子等攻击者攻击的主要对象，哪些网络、系统、平台、数据是被攻击的主要目标，建设重点保护对象档案库，为开展重点保护和防范提供支撑。

（3）掌握“攻击路径”，即及时掌握敌对势力、黑客组织、犯罪团伙和不法分子等攻击者的攻击路径、渠道、资源和手段、方法、谋略、技术特征、工具装备等情况，并纳入黑客档案库，为开展网络安全反制和打击提供支持。

（4）及时掌握威胁情报信息，包括针对和利用重要网络系统的网络攻击、入侵控制、渗透破坏、潜伏窃密等行动性、内幕性信息和线索，建设威胁情报库，对威胁情报信息进行综合分析研判、深挖扩线，及时预警网络安全重大威胁和风险，为开展网络安全防范提供支持。

（5）将获得的威胁情报及时报送公安机关、行业主管部门和重点单位，为打击网络违法犯罪和重要领域网络安全防御提供支撑。

（6）在开展网络安全威胁情报过程中，加强威胁情报力量建设、共享机制建设、技术手段建设，不断积累和提高网络安全威胁情报工作能力和水平。

1.1.4　网络安全威胁情报观的共识

综观古今中外的种种情报学说可知，任何一个组织/机构/政权为了达成某种战略目标，都需要成立专门的组织，持续不断地收集关于己方及他方的信息、数据和知识，并且对这些信息、数据和知识进行分析与研判，从而辅助决策。这个过程就是情报产出和发挥作用的过程。

网络安全威胁情报同样适用于这个过程。在当今时代，信息产业化、产业信息化和数字化、智慧化进程明显加快，云计算、大数据、5G（Fifth-Generation，第五代移动通信技术）、物联网等信息通信技术在各行各业都有越来越广泛的应用。以上态势为互联网增加了更多无形的威胁和风险。大到一个国家，小到一个商业公司，为了保障自身的网络安全，必须通过某些途径从自身与互联网中收集关于己方和攻击者的信息，并通过某些工具或人员进行分析研判，从而辅助自身的安全策略与基线调整、安全产品与设备更新迭代等关键网络安全决策。

探讨网络安全威胁情报观，应达成以下几点共识。

（1）网络安全威胁情报需要为目标组织服务；

（2）网络安全威胁情报的持续运营需要借助专门组织的力量，如成立专项工作小组、与第三方机构合作等；

（3）网络安全威胁情报立足现在，面向未来，是动态的、变化发展的；

（4）从事网络安全威胁情报的组织和个人应采用最新信息化手段，不断收集与己方及攻击方相关的数据、信息和知识；

（5）在数据、信息和知识充足、及时的基础上，应做好对网络安全威胁情报的分析研判工作；

（6）网络安全威胁情报应用于辅助网络安全决策，最终让目标组织受益。

1.2 威胁情报的价值

我国十分重视网络安全威胁情报工作，网络安全等级保护制度、关键信息基础设施安全保护制度对威胁情报库、威胁情报系统、威胁情报工作提出了明确要求。此外，威胁情报生产技术已经被写入《中国禁止出口限制出口技术目录》。为什么威胁情报如此重要，我国又缘何坚定地在行业内推进威胁情报的应用和发展？究其原因，在于威胁情报能够有力地守护企业安全、社会公共安全和国家安全。

1.2.1 威胁情报守护企业安全

2017 年 5 月 12 日，勒索软件 WannaCry 借助微软名为“永恒之蓝”的漏洞在世界范围内快速、大规模传播，被感染的计算机会被锁定，受害者无法自行解决，直到支付相应赎金。在 3 天内，有 100 多个国家的 10 万余台计算机被 WannaCry 感染，经济损失惨重。

转折点发生在 5 月 13 日晚间，一位英国研究员发现了 WannaCry 存在一个后门秘密开关域名，如果计算机连接了这个开关域名，则能够解开勒索软件的限制，从而免于被勒索的命运。然而在两天后，WannaCry 的新变种开始被众多网络安全公司捕获，而当时我国的部分地区对已有的开关域名尚无法进行解析。那么，新变种是否也存在开关域名？我国部分地区开关域名无法解析的问题又该如何解决？

我国网络安全公司捕获到了新变种的样本后，立即对其展开研究，发现新变种也存在开关域名，同时，可以通过添加内网 DNS (Domain Name System，域名系统）解析的方式让开关域名顺利被解析。在反复确认过相关威胁情报后，网络安全公司第一时间将威胁情报同步给一些企业客户。事后统计发现，在这场大范围无差别勒索病毒攻击中，一些获得并采信该条威胁情报的大型企业没有设备遭受勒索攻击，精准、及时的威胁情报创造了“零失陷、零损失”的奇迹。

1.2.2 威胁情报守护社会公共安全

暗网潜藏于普通互联网之下，无法通过一般搜索引擎或者浏览器访问，具有网站的使用者不可被追踪、网站的访问者不可被追踪的特点，其匿名性和保密性极强，因此成为犯罪活动的温床，暗网网站上交易的往往是一些非法内容和商品。

针对暗网领域的违法犯罪乱象，全国公安机关开展专项打击行动。某市警方与知名网络安全公司建立合作关系，充分整合警企技术优势，重拳出击，成功捣毁了一个架设在暗网中的有害网站，成为我国首次破获涉暗网平台的案件。本案中的有害网站架设在暗网中，调查取证难，追踪溯源难，网络安全公司通过暗网监控发现重要线索，生成高可信度

的威胁情报，并辅助专案组进行追踪溯源，有力地支撑了案件侦办。

1.2.3　威胁情报守护国家安全

在全球范围内，具备国家背景的黑客组织会向与己方地缘政治密切相关的国家发起高级持续性威胁（Advanced Persistent Threat，APT）攻击，这类黑客组织被称为 APT 组织，其攻击目的往往是窃取关键行业、领域的敏感信息数据。威胁情报的兴起，对防护 APT 组织的攻击有着重要的积极作用。

2020 年 1 月中旬，“2019-nCoV”新型冠状病毒性肺炎大规模流行，在疫情阻击战时期，一些黑客组织借助疫情热点频繁对目标行业单位发起网络攻击，APT 组织“白象”就是其中之一。“白象”又名 Patchwork、摩诃草、the Dropping Elephant，是一个具有国家背景的 APT 组织。根据掌握的威胁情报，Norman 安全公司于 2013 年曝光了该黑客组织，其主要针对中国、巴基斯坦等亚洲地区国家进行网络间谍活动，以窃取敏感信息为主，相关攻击活动最早可以追溯到 2009 年 11 月。

自 2009 年至今，“白象”组织已经活跃十年有余，从最初的小黑客团伙到如今历经三代，成为一个极具代表性的网络黑客组织。2020 年 1 月中旬，借助“2019-nCoV”热点事件进行定向 APT 攻击是“白象三代”极具代表性的攻击事件，我国于第一时间对具体攻击活动进行披露。通过对该次攻击活动中的网络资产进行深度关联扩线，成功发现该组织自 2019 年 11 月起对我国发起了数次攻击活动，而围绕这些攻击活动又可以追溯到其于 2019 年 3 月中旬发起的钓鱼活动。

此次借助疫情对我国发起的网络攻击活动被我国外交部公开后，nhc-gov.com、moe-cn.org 等域名立即停止解析，标志着“白象三代”的本次攻击活动也进入尾声。威胁情报又一次成功发挥作用，守护了我国国家安全。然而，具备国家背景的黑客组织对我国的攻击渗透活动不会停歇，我国也将继续加强威胁情报工作，在维护国家安全中发挥更大作用。

1.3　威胁情报分析与挖掘的相关概念

威胁情报分析与挖掘是网络安全领域的一个重要内容，它涉及从大量数据中提取、分析和理解与安全威胁相关的信息。这一过程不仅包括对已知威胁的识别，也包括对未来潜在威胁的预测和准备。

1.3.1　威胁情报分析与挖掘的过程

威胁情报分析与挖掘的过程通常包括以下几个关键步骤。

（1）采集与融合：首先需要从各种来源收集数据，然后将这些数据进行整理和融合，以确保信息的准确性和完整性。

（2）分析与挖掘：通过对收集到的数据进行深入分析和挖掘，识别出潜在的安全威胁和模式。这一步骤可能涉及先进的数据分析技术，如机器学习和人工智能算法等。

（3）共享与交换：将分析和挖掘的结果与其他安全实体共享和交换，以促进相互间的联合防御能力。

（4）应用与服务：将分析结果应用于实际的安全防护措施中，帮助组织识别和防御安全威胁。

1.3.2 威胁情报分析与挖掘的技术和方法

随着技术的发展和威胁环境的变化，威胁情报的分析与挖掘方法也在不断演进，但始终不变的是其核心目的——提高组织的安全防护能力和响应速度。威胁情报分析与挖掘中使用的最新技术和方法主要包括以下内容。

（1）智能威胁分析技术：通过知识图谱和深度学习方法来分析 APT 攻击并提高防御能力。包括数据处理技术、威胁建模、表示、推理方法等方面内容。

（2）大数据技术：依托微服务、分布式集群、海量数据存储、消息队列等大数据软硬件基础组件，构建底层大数据架构。使用 ElasticSearch、Hadoop、Spark、Kafka 等开源分布式技术，解决海量数据接入、解析、分析、存储、输出等关键环节。

（3）机器学习和自然语言处理技术：对收集到的威胁情报进行深度分析，提取高价值的战略情报和战术情报。

（4）AI（Artificial Intelligence，人工智能）算法：利用 AI 技术生成 AI 算法，提供实时威胁分析功能，从而更快、更精准地应对网络攻击事件。

这些技术和方法的应用，使得威胁情报分析与挖掘能够更加高效、准确地识别和响应网络安全威胁，为网络安全防御提供强有力的支持。

1.3.3 威胁情报分析与挖掘的效果评估

评估威胁情报分析与挖掘的效果和准确性，可以从多个维度进行考量。

（1）一个有效的威胁情报分析工具或方法应当能够全面覆盖这些方面，确保提供的情报既全面又准确。

（2）时效性是威胁情报的一个重要特征，发布时间是评价威胁情报是否有效的重要指标之一。因此，评估威胁情报的效果时，需要考虑情报的更新频率和时间敏感性，即威胁情报的时效性。

（3）通过非量化的标准和指标为开源威胁情报的质量提供全面的评估框架。这表明，在评估过程中，除了定量分析，还需要结合定性的评估方法，以识别威胁情报的关键特征

和价值。

（4）通过数学计算来度量风险程度，为不同来源的威胁提供统一标准。这种方法有助于客观地评估威胁情报的准确性和实用性。

（5）在评估威胁情报的效果和准确性时，还需要考虑威胁情报来源的多样性和可靠性。

评估威胁情报分析与挖掘的效果和准确性是一个多维度的过程，需要综合考虑威胁情报的完整性、一致性、准确性、及时性、时效性，以及情报来源的多样性和可靠性等多个方面。

1.3.4　威胁情报分析与挖掘的策略

面对新型威胁，威胁情报分析与挖掘的策略主要包括以下几个方面。

（1）战术级威胁情报的应用：通过收集、分析以及利用失陷指标（Indicators of Compromise，IOC）、攻击者技战术与攻击流程，来提升机构整个安全环境的检测与防御能力。这要求对威胁情报进行有效的整合和应用，以提高应急响应效果并降低安全事件的影响。

（2）威胁情报综合分析系统的建设：基于海量流量侧和端点侧威胁感知能力，结合自动化样本采集分析体系，形成高质量的自有威胁情报库和威胁知识库。这种系统能够提供内外部情报的结合，增强威胁情报的准确性和实用性。

（3）高级威胁情报的聚类与攻击者分析：从 UEBA（User and Entity Behavior Analytics，用户行为分析）视角出发，进行情报聚类分析，帮助安全管理者从完整攻击者画像的角度审视高级威胁情报。这种方法有助于识别与理解攻击者的模式和行为，从而更有效地预防和应对威胁。

（4）开源异构数据的威胁情报挖掘：基于威胁情报命名实体识别（Threat Intelligence-Named Entity Recognition，TI-NER）算法，从开源网络安全报告中高效挖掘威胁情报。这种方法可以提高威胁情报的质量和可信性，能够为后续的威胁情报和威胁攻击的关联挖掘提供输入线索。

（5）多源情报汇聚与 APT 事件追踪：通过覆盖安全数据上下文关联、网络威胁分析等场景的安全星图平台，帮助用户应对已知与未知威胁。这种平台能够提升用户对网络安全风险的溯源分析能力，增强对新型威胁的识别和响应能力。

（6）自动化威胁情报服务：利用自动化的威胁情报服务，如大型互联网企业提供的服务，可以对威胁指标进行分级、威胁信息上下文关联和数据分析。这种服务支持相关人员读取威胁情报并对其进行处置，提高处理速度和效率。

面对新型威胁，威胁情报分析与挖掘的策略涉及多个方面，包括但不限于上述内容，应用好这些策略能够帮助机构更好地识别、预防和应对新型威胁。

1.3.5 威胁情报分析与挖掘过程中的挑战和解决方法

威胁情报分析与挖掘过程中的挑战包括但不限于数据收集的难度、信息的准确性、以及如何有效地利用这些情报以提高安全防护能力。解决方法则涵盖了从技术手段到策略方法的多个方面。

（1）数据收集的挑战：在威胁情报的收集过程中，面临的一个主要挑战是如何有效地收集到有价值的数据。这可能涉及网络攻击的技术细节、攻击者的动机和目标等多个维度。为了解决这一问题，可以采用基于 APT 攻击的情报挖掘方法，通过深入分析 APT 的情报学价值，探析 APT 情报挖掘方法，从而更好地服务于情报机构。

（2）信息的准确性：确保收集到的信息准确无误是另一个重要挑战。错误的信息可能导致错误的安全决策，从而增加安全风险。AI（人工智能）技术的应用被认为是解决这一问题的有效手段之一。根据全球知名 IT 媒体 TechTarget 旗下企业战略集团（Enterprise Strategy Group，ESG）的调查，大多数的企业计划增加威胁情报支出，并借助生成式人工智能的力量来消除企业面临的威胁情报痛点。

（3）有效利用情报：即使成功收集并验证了威胁情报，如何有效地利用这些情报以提高安全防护能力也是一个挑战。一种解决方案是结合主动学习的威胁情报 IOC 识别方法，这种方法可以在一定程度上降低数据标注成本，提高情报利用的效率。

（4）共享和协同：威胁情报的有效共享和协同也是提高整体网络安全的关键。当前，威胁情报的效用有待提高，其本质是威胁情报的供给和消费能力频谱始终滞留在文件 Hash（Hash，即哈希，或称为散列算法，文件 Hash 是对文件内容进行特定的 Hash 运算得到的固定长度的唯一标识符）、IP（Internet Protocol，互联网协议）地址等基础层面。因此，需要强化威胁情报的共享和协同来应对日益严峻的威胁挑战。

（5）技术和策略方法：为了提高威胁情报的利用效率和质量，可以采用全新的动态利用方式，这种方式可以充分挖掘情报的价值。通过与现有安全解决方案或安全运营体系相结合，最大限度筛选安全数据、减少警报疲劳、优化安全防护措施。

威胁情报分析与挖掘过程中的挑战多样，解决方法也应多方面考虑，包括但不限于采用先进的技术手段、加强信息的准确性、有效利用情报、促进情报的共享与协同，以及结合策略方法提高整体的安全防护能力。

习　题

1．孙子兵法的情报思想包含哪两个部分？

2．美国情报理论先驱谢尔曼·肯特曾在《服务于美国世界政策的战略情报》一书中对情报提出哪三个定义？

3．开展网络安全威胁情报工作的原则是什么？
4．在探讨网络安全威胁情报观时，应达成哪些共识？
5．威胁情报分析与挖掘的过程通常包括哪几个关键步骤？
6．威胁情报分析与挖掘过程中，使用的最新技术与方法主要包括哪些？
7．简述威胁情报分析与挖掘的策略。
8．威胁情报分析与挖掘过程中，如何收集到有价值的数据？
9．威胁情报分析与挖掘过程中，如何保障和提升数据的准确性？